read；不是很清晰
基于检测的方案；
把交互节点的自私行为建模为贝塔分布，根据K-Means方法和推荐相似性进行推荐信息的融合，采用贝叶斯决策理论在分布式场景中估计和判定其他节点是否进行自私行为。

ReFIoV: A Novel Reputation Framework for Information-Centric Vehicular Applications

Naercio Magaia and Zhengguo Sheng

***Abstract*—In this paper, a novel reputation framework for information-centric vehicular applications leveraging on machine learning and the artificial immune system (AIS), also known as ReFIoV, is proposed. Specifically, the Bayesian learning and classification allow each node to learn as newly observed data of the behavior of other nodes become available and hence classify these nodes, meanwhile, the k-means clustering algorithm allows us to integrate recommendations from other nodes even if they behave in an unpredictable manner. The AIS is used to enhance misbehavior detection. The proposed ReFIoV can be implemented in a distributed manner as each node decides with whom to interact. It provides incentives for nodes to cache and forward others' mobile data as well as achieves robustness against false accusations and praise. The performance evaluation shows that ReFIoV outperforms state-of-the-art reputation systems for the metrics considered. That is, it presents a very low number of misbehaving nodes incorrectly classified in comparison with another reputation scheme. The proposed AIS mechanism presents a low overhead. The incorporation of recommendations enabled the framework to reduce even further detection time.**

***Index Terms*—Reputation, routing, caching, Bayesian learning, danger theory, vehicular delay-tolerant networks.**

I. Introduction

THE forthcoming vehicular network infrastructure is going to increase the ubiquitousness of the Internet and the general connectivity by incorporating every object and forming an intelligent vehicular transportation system (ITS). Using advanced vehicular communications, that is, vehicle-to-everything (V2X), research communities have the possibility of reaching a comprehensive variety of objectives efficiently. Examples of vehicular applications for such a promising combination ranges from providing assistance to drivers and road safety, to mapping road status and multimedia content sharing. However, the amount of data required for such applications will continue to increase along with the need to minimize latency as a result of an increasing number of connected vehicles as well as more evolved use cases. Although the amount of data stored and processed centrally may be adequate for some non-critical use cases, it can be unreliable and slow, particularly when a large number of vehicles try to access a given service at the same time.

The development of 5G mobile technology enables broad coverage and high bandwidth to provide multimedia content downloading services for the moving vehicles, even though most probably being overloaded and congested especially during peak times and in urban central areas with the increase of the services and user demands [1]. Consequently, 5G-based vehicular communications will face extreme performance hits in terms of low network bandwidth, missed calls, and unreliable coverage. However, the opportunistic contacts enabled by V2X communications can provide high bandwidth for the transmission of data as well as enable vehicles to build relationships with other objects they might come into contact, which forms the basis of Information-Centric Internet of Vehicles (I^2oV).

Motivated by content caching at the edge of 5G networks (e.g., at the Radio Access Networks - RANs) that would help relieve backhaul congestion and meet peak traffic demands with lower service latency, service providers can postpone a big number of data transmissions to an I^2oV consisting of a 5G-based Vehicular Delay-Tolerant Networks (VDTNs) [2]. That is, use in-network caching, by benefiting from the delay-tolerant feature of some non-real time vehicle applications. Albeit the VDTN approach may cause an acceptable delay in the dissemination of data, it assists in handling the volatile traffic demands and foreseen mobile data increase currently and in the near future. Vehicular applications such as Wireless Remote Software Updates (WRSUs) and traffic map updating, are one of the most critical challenges in the automotive ecosystem and can benefit from such I^2oV. Even though routing protocols have been proposed in the literature for VDTNs [3], several stimulating research problems exist in providing efficient data access to moving vehicles, despite the importance of data accessibility in many mobile applications. Therefore, appropriate network design and/or incentive schemes are needed to ensure that data can be promptly accessed by requesters in such cases.

Cooperative caching in VDTNs allows for allocation and coordination of cached data between nodes and to reduce delay to access data. In addition, and according to [4], an information-centric approach is well suited to the nature of usual vehicular

Manuscript received June 18, 2018; revised October 27, 2018 and December 6, 2018; accepted December 10, 2018. Date of publication December 13, 2018; date of current version February 12, 2019. This work was supported in part by the Engineering and Physical Sciences Research Council (EP/P025862/1), in part by the Royal Society-Newton Mobility Grant (IE160920), in part by H2020 European-Pacific Partnership fund, and in part by the LASIGE Research Unit, UID/CEC/00408/2013. The review of this paper was coordinated by Dr. S. Zhong. *(Corresponding author: Naercio Magaia.)*

N. Magaia is with the Department of Engineering and Design, University of Sussex, Falmer BN1 9RH, U.K., and also with the Large-Scale Informatics Systems Laboratory (LASIGE), Faculdade de Ciências, Universidade de Lisboa, Lisboa 1749-016, Portugal (e-mail: N.Magaia@sussex.ac.uk).

Z. Sheng is with the Department of Engineering and Design, University of Sussex, Falmer BN1 9RH, U.K. (e-mail: Z.Sheng@sussex.ac.uk).

Digital Object Identifier 10.1109/TVT.2018.2886572

applications as these applications benefit from in-network and distributed replication mechanisms for data caching. Content caching is also beneficial for intermittent on-the-road connectivity and can speed up data retrieval through content replication in several nodes. Neither Information-Centric Networking (ICN) [4] nor VDTN relies on the paradigm of end-to-end communications, but both rely on in-network storage. However, nodes in such environments might misbehave due to the fact of them being controlled by rational entities. *Node misbehavior* can affect meaningfully the performance of the network [5].

Routing as well as caching decision-making becomes much easier when reputation and trust are used. Reputation systems [6] are those where each node uses other nodes reputation when deciding to interact. In a distributed reputation system, ratings of nodes are kept in a decentralized manner and the evaluation of reputation is based on parts of information. Thus, this article proposes a novel reputation framework for information-centric vehicular applications such as content dissemination. ReFIoV utilizes machine learning [7] and artificial immune system (AIS) [8] techniques to address the data accessibility problem, i.e., the routing problem of vehicular delay-tolerant applications as well as the caching problem of information-centric vehicular applications by providing incentives and hence stimulating nodes' cooperation.

The contributions of this article are summarized as follows:

- ReFIoV, a novel reputation framework, which leverages Bayesian learning, K-Means clustering, and Danger Theory to provide incentives for caching in information-centric approaches as well as routing in vehicular delay-tolerant approaches aiming at improving data accessibility of the moving vehicles, is proposed. ReFIoV presents a very low number of misbehaving nodes incorrectly classified.
- A personalized similarity metric that determines the difference in opinions resulting from direct experiences over a common set of interacting nodes is proposed. It is used to cluster nodes using the K-Means Clustering algorithm, which allows integrating other nodes' recommendations hence making the framework resilient against false accusations and praise as a result of an unpredictable nodes' behavior. The integration of recommendations reduces in further our framework's detection time.
- A biologically inspired mechanism from AIS to enhance misbehavior detection is proposed. The additional overhead caused by the mechanism is low.

It is our convictions that the use of incentive schemes in I^2oV applications is yet an open research problem hence addressed in this article.

The remainder of this paper is as follows. Section II presents related work. Section III presents preliminaries and background. Section IV presents the ReFIoV scheme. In Section V, the performance evaluation of ReFIoV is presented. Finally, Section VI presents concluding remarks and future work.

II. Related work

A. ICNs

ICNs [1], in contrast to the host-centric paradigm that is based on perpetual connectivity and the end-to-end principle, focus on the distribution and retrieval of "named information" (that is, content or data). ICN is based on the publish-subscribe paradigm and the concepts of naming and in-network caching. Content may be distributed either in caches along the delivery path(s) or in any cache within the network. Network connectivity may also be intermittent in ICNs. Therefore, there are clear synergies between ICNs and VDTNs [9] as both do not depend on the paradigm of end-to-end communications. Specifically, both approaches rely on in-network storage, adopt late binding of names to locations because of the possibly big interval among the generation of request and response, and consider that data can be present in the network for prolonged time periods. Nevertheless, there are cases where the information-centric paradigm is not suitable for use in vehicular delay-tolerant environments such as when information is not the main communication object transmitted, and when a single destination is continuously used for the reception of information, which may not guarantee that independent information objects are identified and routed. In summary, ICN can be used to enhance VDTN's data dissemination and traffic monitoring applications leveraging on mobile cloud and social networking.

B. Reputation-Based Incentive Schemes

The use of reputation-based incentive schemes has been extensively studied in wireless networks such as Mobile Ad Hoc Networks (MANETs) and is under research in VDTNs and ICNs. Reputation-based routing protocols for MANETs benefit from existing end-to-end routing paths between a source and destination nodes to monitor routing behaviors of intermediate nodes along those paths, conversely to VDTNs that are characterized by long and variable delays, high error rates, and intermittent connectivity. For instance, the watchdog (or monitor), on the one hand, is used at the source node to count the arrival of ACKs associated with data packets that were sent as an indicator of good behavior of intermediate nodes. On the other hand, it is used to monitor directly wireless channels to check if the next-hop node properly forwarded the data packet. However, since end-to-end connectivity between a source and destination nodes might never exist, the success probability of techniques such as channel monitoring or end-to-end ACKs in VDTNs is much lower than for MANETs.

Some reputation-based incentive schemes have been proposed for DTNs and VDTNs. The authors of [10] proposed a cooperative watchdog system aiming at supporting selfish nodes detection in VDTNs. A reputation score is assigned to a node whenever it takes part in a contact opportunity. As new observations are made, the proposed classification module does not learn. The authors of [11] proposed a reputation-based extension to the Context-Aware Routing [12] protocol to address the problem of black-holes. The cooperation evaluation phase is dependent on the reception of acknowledgment messages.

In [13], [14], Bayesian approaches leveraging on the Dempster-Shafer Belief Theory [15] were proposed. The trust-based framework proposed in [13] can be integrated with single-copy data forwarding protocols. It uses a watchdog component and a special message to monitor the forwarding behavior of a node. If sparse DTNs are considered, the proposed special

message will take a longer time to reach its intended node, hence, not being suitable. In [14], which is similar to [16] in the sense that each node also manages evidence of its reputation and shows it whenever necessary, two concepts have been introduced, namely self-check and community-check. They were defined for reputation evaluation in relation to the forwarding competency of the candidate and the sufficiency of the evidence that the node presents, and for speeding up reputation establishment and forming consensus views towards targets in the same community. This approach presents a slow convergence.

The authors of [17] proposed a reputation mechanism for opportunistic networks that uses social-network information to detect and penalize misbehaving nodes, therefore, stimulating them to participate in the network. In [18], [19], social trust routing schemes were proposed. In [18], the trust routing based on social similarity scheme is built on the observation that nodes move around and contact each other according to their common interests or social similarities. In [19], the social trust model exploits the contact status, forwarding ability, and common attributes. In addition, a trust-based routing algorithm and buffer management algorithm for the secure routing strategy that considers network coding in data dissemination was also proposed. The approaches in [17]–[19] are limited to social-based DTNs.

The authors of [20] proposed a probabilistic misbehavior detection scheme for secure routing. A trusted authority, which is periodically available, judges nodes' behavior based on the collected routing evidence and performs probabilistic checks. A trusted third party to judge and punish nodes based on their behavior is required. In [21], a distributed mechanism for malicious node detection and iterative trust management were proposed. It uses an iterative trust and reputation mechanism that enables each node to evaluate others based on their past behavior. This approach presents large communication overhead in order to gather sufficient rating information in DTN environments.

In [22], a previous work of ours, a changed Bayesian approach for representation and update of reputation and trust, and for integration of second-hand information was proposed for DTNs. It evaluates the participation of each node in the network as well as each node honesty is in the reputation system. In [1], a robust and distributed incentive scheme for collaborative caching and dissemination in content-centric cellular-based Vehicular Delay-Tolerant Networks was proposed. Despite both addressing different problems, that is, providing incentives for routing [22] and in-network caching [1], it is unclear the advantages of using second-hand information in these approaches. Their performance evaluation was not exhaustive and these approaches were not compared with state-of-the-art reputation systems. Furthermore, the evaluation of [1] did not consider queries generation patterns that are common in content distribution applications.

On the other hand, ReFIoV is a novel reputation framework for information-centric vehicular applications such as content dissemination. It leverages on AIS to enhance misbehavior detection. The performance evaluation considered a much more elaborate attack where colluding vehicles oscillated their behavior over time. In addition, more simulation scenarios were considered, and ReFIoV was compared to state-of-the-art reputation systems. The majority of previous works only proposed incentive schemes for routing in DTNs and VDTNs. With the overwhelming increase in the volume of data required by 5G vehicular applications, incentives for content dissemination are crucial hence proposed in this article. Providing incentives to information-centric vehicular applications is yet an open research problem.

III. Preliminaries and Background

A. Assumptions and Notations

a) Notation: A notation similar to [23] is used. A VDTN is modeled as a time-varying graph $\mathcal{G} = (V, E, \mathcal{T}, w)$ where each vertex $v \in V$ corresponds to a node in the network and each edge $e = (i, j) \in E$ represents the relationship between these nodes (i.e., that these nodes have encountered before). The relations among nodes are assumed to take place over a time span $\mathcal{T} \in \mathbb{T}$ known as the lifetime of the network; $w : E \times \mathcal{T} \rightarrow [0, 1]$ is called *weight* function and indicates the strength of an edge at a given time.

time窗口，图G的footprint序列

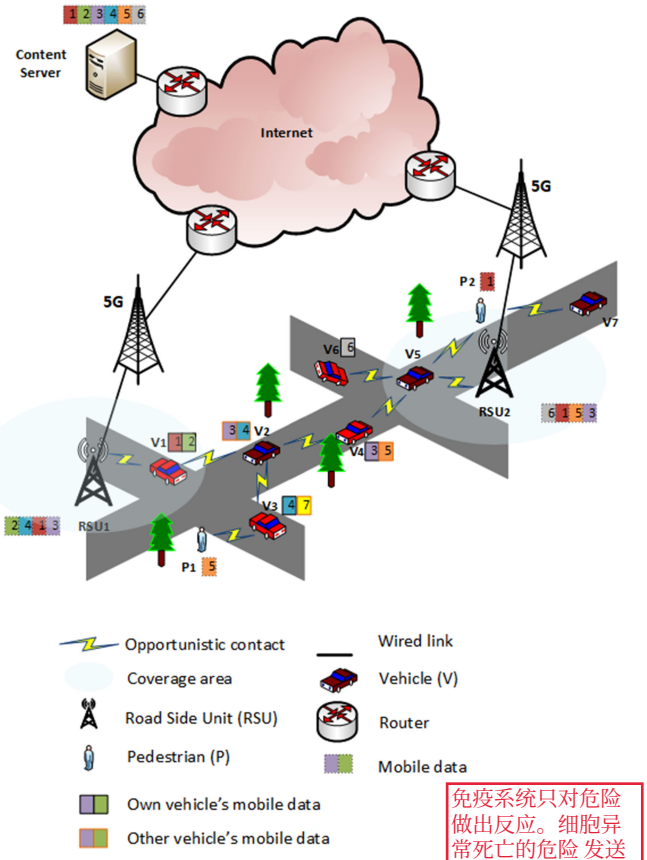
Let a footprint of $\mathcal{G}$ from t_1 to t_2 be defined as a static graph $G^{[t_1,t_2)} = (V, E^{[t_1,t_2)})$ such that $\forall e \in E, e \in E^{[t_1,t_2)} \iff \exists\ t \in [t_1, t_2), \quad w(e, t) \in [0, 1]$, i.e., the footprint aggregates all interactions of a given time window into static graphs. Let $\tau = [t_0, t_1), [t_1, t_2), \ldots, [t_i, t_{i+1}), \ldots$ (where $[t_k, t_{k+1})$ can be noted τ_k) be the lifetime $\mathcal{T}$ of the time-varying graph partitioned in sub-intervals (or time-slots). The sequence $\mathrm{SF}(\tau) = G^{\tau_0}, G^{\tau_1}, \ldots$ is called sequence of footprints of $\mathcal{G}$ according to τ.

Let $H = (V_H, E_H)$ be a subgraph of $G = (V, E)$, denoted $H \subset G$, if and only if $V_H \subset V$ and $E_H \subset E$. H is a local subgraph with respect to a vertex $v \in V$, if and only if all vertices in the subgraph can be directly reached from v.

b) Scenario: Consider the network topology in Fig. 1, where vehicles and pedestrians move around the city and the set up RSUs provide coverage over a certain area. RSUs are positioned at road intersections similarly to what is done by current optimal placement algorithms [24]. RSUs and pedestrians are connected through wired and wireless links to 5G RANs, respectively, which are also connected to the content server on the Internet. Vehicles needing mobile data such as software or traffic map updates can send their requests to the content server via V2X communication links. The content server sends the requested data to the 5G RAN, and from the 5G RAN to the RSUs and pedestrian via the wired and wireless links, respectively. It is assumed that the wired links make available high bandwidth hence ensuring that the requested data is delivered to RSUs prior to the opportunistic communication between RSUs and vehicles. The data will additionally be disseminated to the users in the vehicles that requested it through opportunistic communication that occurs when the vehicle moves into the communication coverage of RSUs or pedestrians. Please note that the words vehicle and node are used interchangeably throughout the article.

c) Node Capability: Each node has a Unique IDentifier, and it cannot be spoofed. Upon an encounter between two nodes, a secure communication channel between the two is used through cryptographic mechanisms that ensure confidentiality.

另外一个节点实际存储的内容是根据自己的兴趣；无法进行限制；
类似于black-hole 节点丢弃其他节点感兴趣的node



免疫系统只对危险做出反应。细胞异常死亡的危险 发送出来

Fig. 1. An illustration of an I^{2}oV content dissemination application integrating a 5G network and V2X opportunistic communications.

d) Attack Model: In the I^{2}oV scenario depicted in Fig. 1, vehicles, pedestrians and RSUs decide which contents to cache and, for example, the RSUs proactively fetch these contents via backhaul during off-peak times, and transmit the contents to requesters during peak times. As a result, caching offloads the network traffic during peak times and reduces vehicular users' average delay cost.

The 5G RAN aims to minimize its traffic load of serving nodes by reducing the backhaul load and the transmission cost. This objective is equivalent to maximizing the chances of V2X communications in the network. The vehicles' malicious nature hence becomes the major obstacle for the 5G RAN to achieve its objective. In an I^{2}oV of misbehaving vehicles (i.e., malicious or socially selfish) as vehicles are owned or managed by rational entities, each vehicle (or group of vehicles) cares solely about the contents of its users. Specifically, each vehicle only intends to cache the favorite contents of its users hoping also that its neighbors can cache as many as possible favorite contents of its users. Specifically, there are 6 contents $\{1, 2, 3, \ldots, 6\}$ on the content server of Fig. 1. It is assumed that each content is of a unitary size and the local cache of each vehicle be able to store two contents. It is also assumed that the ranking of content preferences of the users in vehicle V_1 and V_5 are $(1, 2, \ldots, 6)$, $(6, 5, \ldots, 1)$, respectively. Certainly, V_1 will cache contents $\{1, 2\}$ wishing also that its neighbors will cache contents $\{3, \ldots, 6\}$ whereas V_5 will cache contents $\{6, 5\}$ hoping that its neighbors will cache contents $\{4, \ldots, 1\}$. The latter resembles a *black-hole attack* as each vehicle will most probably discard the contents of other vehicles. A similar, however much more elaborate attack, is the *gray-hole attack*, where each vehicle oscillates its behavior over time by caching and discarding other vehicles' contents. Black and gray-hole attacks may cause duplicate caching and under-utilization of the storage space for all vehicles. Therefore, the 5G RAN would be overloaded by vehicles' requests and vehicles would suffer from larger delays. In addition, active attacks, which are characterized by an unauthorized party modifying the contents of the message, are not considered because the wireless network's cryptographic techniques perform well under active attacks.

AIS生物免疫系统，通过分布式、智能化的帮助，本地和全局平均状况下

B. Background

1) Danger Theory: The biological immune system [25] is a robust, complex and adaptive system, which has evolved over millions of years, hence protecting the body from foreign pathogens. It is able to classify the cells in the body as self-cells or non-self (or foreign) cells. It achieves this with the assistance of a distributed and intelligent task force that takes action from a local and global viewpoint by means of its network of messengers for communication.

AIS is a novel computational intelligence technique that is inspired from immunology. Over the years, several concepts from immunology have been extracted and applied for the solution of real-world science and engineering problems.

According to classical immunology [25], an immune response is activated if something non-self is encountered in the body. Danger theory [8] offers a way of grounding the immune response. According to the theory, the immune system does not respond to non-self but to danger. That is, the immune system reacts to danger instead of responding to foreignness. The damage to cells indicated by affliction signals that are sent out when cells die an abnormal death, conversely to planned cell death, enables to measure danger. Antigens in the vicinity are caught by antigen-presenting cells when an alarm signal is sent out by a cell in distress. In essence, a danger zone is established around the danger signal. Therefore, white blood cells that produce antibodies matching antigens in the danger zone become stimulated and go through the process of clonal expansion, and do not get stimulated the ones that are too far away or do not match.

2) Machine Learning: Machine learning (ML) is set of techniques that detect patterns in data by design. The discovered patterns are used to forecast future data or to perform additional types of decision making under uncertainty. The two main fields of ML are supervised and unsupervised learning. Supervised learning focuses on exact prediction, e.g., Bayesian learning, whereas unsupervised learning aims to find compact descriptions of the data, e.g., K-Means clustering.

a) Bayesian decision theory: Some fundamental concepts of the Bayesian decision theory [26] are:

- All that is unknown but relevant for making a decision is represented by θ and takes values on a state space Θ. The available knowledge about θ, *prior*, is characterized by its

probability function $\pi(\theta)$. Hereafter, it is considered that Θ is discrete.

- The *observed data*, x, which are used to make decisions, are most likely random depending on θ. This dependence is expressed assuming that x is a sample of a random variable $X \in \mathcal{X}$ whose probability function is conditioned on θ, i.e., $f(x|\theta)$ that is also known as the *likelihood function.*
- A *decision rule* $\delta(x)$ has to choose an action amongst a set $\mathcal{A}$ of allowed decisions or actions. $\delta(x)$ is a function from $\mathcal{X} \rightarrow \mathcal{A}$ thus specifying how actions or decisions are chosen given x. $\mathcal{D}$ is the set of allowed decision rules.
- A *loss function* $L(\theta, a) : \Theta \times \mathcal{A} \rightarrow \mathbb{R}$, specifies the cost incurred if the unknown parameter is θ and the chosen decision is a, thus quantifying the consequences of the decisions.

A Bayesian decision problem can be formalized by the set of elements $\{\Theta,\ \pi(\theta),\ \mathcal{A},\ \mathcal{X}, L(\theta, a), \mathcal{D},\ f(x|\theta)\}$ and is considered solved if a decision rule $\delta(x)$ is chosen in a way to obtain some kind of optimality criterion that is associated with the loss function.

In Bayesian decision theory, the *posterior* expected loss, conditioned on observed data x, is defined as

$$\rho(\pi(\theta), a|x) = \mathbb{E}[L(\theta, a)|x] = \sum_{\theta \in \Theta} \pi(\theta|x) L(\theta, a) \quad (1)$$

whereas via Bayes law,

$$\pi(\theta|x) = \frac{f(x|\theta)\pi(\theta)}{\sum_{\theta \in \Theta} f(x|\theta)\pi(\theta)} \quad (2)$$

where $\pi(\theta)$ is the prior density of θ, $\pi(\theta|x)$ is posterior density for θ given x, $f(x|\theta)$ is the likelihood for θ based on x so that in terms of θ, $posterior \propto likelihood \times prior$.

b) K-Means clustering: Clustering is the process of grouping alike objects together. In similarity-based clustering, the input to the algorithm is an $N \times N$ dissimilarity matrix or distance $\mathbf{D}$. Similarity-based clustering allows for easy inclusion of domain-specific similarity functions. A dissimilarity matrix $\mathbf{D}$ is a matrix where $d(a, a) = 0$ and $d(a, b) \geq 0$ is a measure of "distance" between objects a and b. Some common attribute dissimilarity functions are

- Squared (Euclidean) distance: $d(a, b) = \|a - b\|^2$
- l_1 distance: $d(a,) = |a - b|$

The K-Means algorithm works as follows: given an initial set of K means, each observation is assigned to the cluster whose mean has the least distance. Then, the new means are calculated to be the centroids of the observations in the new clusters. The assignments no longer change when the algorithm converges.

IV. The ReFIoV Scheme

ReFIoV is a novel reputation framework for information-centric vehicular applications such as content dissemination, leveraging on Bayesian learning and classification, and K-Means clustering of ML and Danger Theory of AIS. ReFIoV is distributed, robust and multi-purpose as it addresses both routing and caching problems. It was built upon our previous work [22]. However, differently from [22] that only addressed the routing problem in delay-tolerant environments, our framework also addresses the caching problem in information-centric vehicular applications. The latter problem is equivalent to two routing problems as there are the query and content dissemination phases. As newly observed data about other nodes become available, Bayesian learning and classification allow the framework to learn and make decisions, meanwhile, K-Means clustering algorithm allows to integrate recommendations for other nodes. Danger theory is used to enhance misbehavior detection.

There are three modules in ReFIoV: the reputation module (that uses Bayesian learning and the biologically inspired mechanism), the trust module (that uses the K-Means clustering algorithm) and the decision module (that uses Bayesian and nearest neighbor classifiers). Fig. 2 shows the block diagram of ReFIoV.

A. The Modified Bayesian Approach

Each vehicle considers that there is a given parameter, θ, such that another vehicle misbehaves with probability θ, and that the outcome is drawn independently at each observed data x. Furthermore, each vehicle considers that there is a different θ for every other vehicle. These parameters are unknown, hence modeled according to $\pi(\theta)$ which is updated as new observations become available.

The beta probability density function $Beta(\theta|\alpha, \beta)$, where $0 \leq \theta \leq 1$ and the parameters $\alpha, \beta > 0$, is used as the prior since it represents probability distributions of binary events (e.g., good or bad) and the conjugate is also a Beta distribution [27]. The Beta density can be expressed as

$$f(\theta|\alpha, \beta) = Beta(\theta|\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} \theta^{\alpha - 1}(1 - \theta)^{\beta - 1} \quad (3)$$

where $0 \leq \theta \leq 1$and $\alpha, \beta > 0$, and Γ is the Euler gamma function defined as $\Gamma(z) = \int_0^\infty u^{z-1} e^{-u} du$ and is valid for any complex number z. The expectation of the Beta density is

$$\mathbb{E}[Beta(\theta|\alpha, \beta)] = \frac{\alpha}{\alpha + \beta} \quad (4)$$

The Bayesian process works as follows. Initially, each vehicle has the prior $Beta(1, 1)$, that is, the uniform distribution on $[0, 1]$, for all its neighbors. The $Beta(1, 1)$ prior represents the absence of information as there are no observations. When a newly observed data is available, if a correct behavior is observed then $x = 1$; otherwise $x = 0$. The prior is updated according to $\alpha_{\text{new}} = \alpha_{\text{old}} + x$ and $\beta_{\text{new}} = \beta_{\text{old}} + (1 - x)$.

Due to the network dynamics, a vehicle may change its behavior over time in contrast to the standard Bayesian framework that gives the same weight regardless of time of occurrence of the observed data. Therefore, old observations may not always be relevant to the most recent ones. The fading mechanism allows forgetting gradually old observations and works as follows

$$y_\eta^\tau = y_\eta^{\tau - 1}\eta + y^\tau \quad (5)$$

where y_η^τ is the accumulated value with fading of a given vehicle at time-slot τ, y^τ is the new value at time τ and η is the fading factor and $0 < \eta < 1$.

节点的错误行为出现概率可能是和time相关的；

但标准Bayesian对不同时间的观察值给了同样的权重

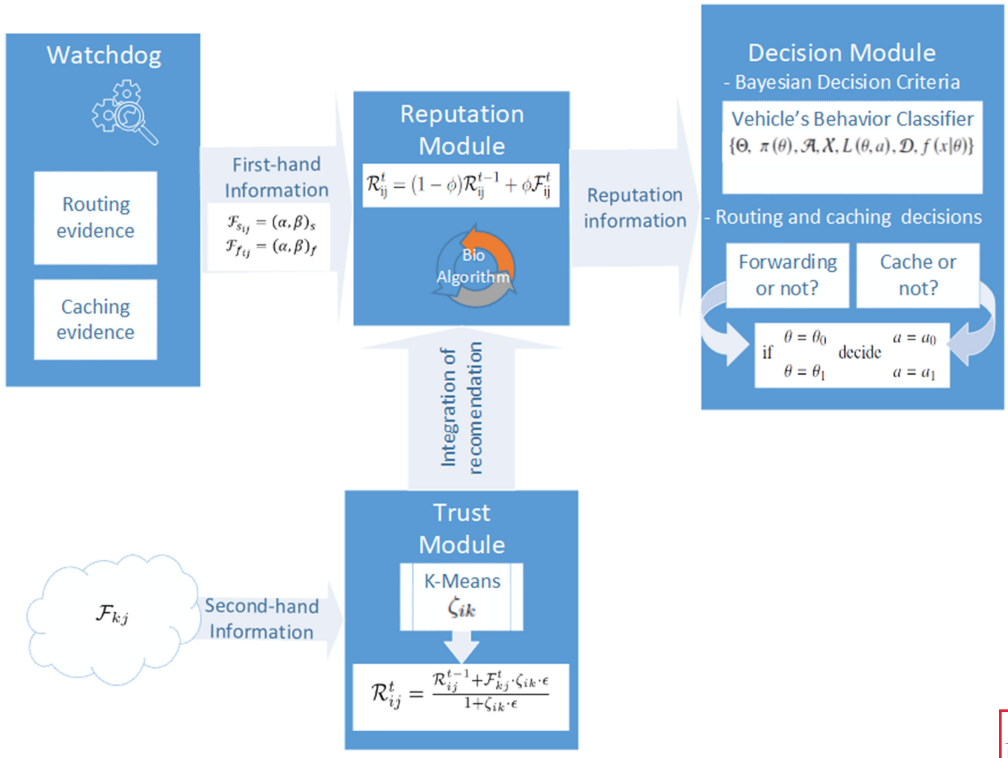


Fig. 2. The block diagram of ReFIoV.

α增加 是 节点j出现正面行为（评价）；β增加则是出现负面行为（评价）

B. Information Gathering

Each vehicle is equipped with a pseudo-watchdog component that allows it to monitor the behavior of the other vehicles with whom it interacts. Specifically, if vehicle v_i forwards mobile data (i.e., query or content) to vehicle v_j, the behavior of v_j is evaluated in terms of two types of evidence, namely: (*i*) if v_j stores data[1] (or caches contents) of v_i and, (*ii*) if v_j forwards (or disseminates) v_i's data to another vehicle, say v_k. The former evidence is collected through direct communication between two vehicles (i.e., through experience), meanwhile, the latter is through *Special Feedback Messages* (SFMs). Therefore, v_i waits for an SFM. SFMs can be forwarded using any routing protocol such as Epidemic routing protocol [28]. However, other dissemination approaches considering social and/or mobility features or predietable trajectories of vehicles could be applied. Two types of SFMs are proposed: (*i*) *type-1* that is created by v_k, which is 2 hops away from v_i (which can be a vehicle that stored (or cached) the data); and (*ii*) *type-2* that is created: (*a*) by the destination of the data or (*b*) by vehicle that requested the data, for the routing and caching problems, respectively. In addition, and uniquely for the caching problem, a *type-2* SFM is also created upon a cache hit. Each SFM contains the mobile data identifier, the list of vehicles that the mobile data traversed and the mobile data digest.

The first-hand information represents the parameters of the Beta distribution assumed by v_i in its Bayesian opinion of v_j's behavior in the system. Each vehicle keeps two data structures (records): *store first-hand information* ($\mathcal{F}_{s_{ij}}$) for stored (or cached) data and *forward first-hand information* ($\mathcal{F}_{f_{ij}}$) for forwarded (or disseminated) data.

For each record, there are two counters: α and β. Store and forward first-hand information is given by $\mathcal{F}_{\mathfrak{x}_{ij}} = (\alpha, \beta)_{\mathfrak{x}}$, where $\mathfrak{x} \in \{s, f\}$, and they are updated to identify *attacks' signature* as follows:

- α is incremented if a good behavior is observed when:
  - v_j stores (or caches) data of other vehicles, e.g., v_i. However, only storing (or caching) others' data may not be optimal for the system, besides being an indicator of a misbehavior such as a *black-hole attack*. Therefore, it is also necessary to ensure that v_j forwards (or disseminates) data that it stores (or caches) if the data was not requested by it; or
  - v_i receives an SFM from v_k because of the data v_i forwarded (or disseminated) to v_j.
- β is incremented if a misbehavior is observed when:
  - vehicle v_j not being the destination or requester of the data forwarded by v_i, did not forward (or disseminate) this data (no SFM was received neither did the data Time-To-Live (TTL) expire); or
  - v_j did not store (or cache) data of other vehicles, e.g., v_i. v_j can only refuse to store (or cache) data forwarded (or disseminated) to it, if it already has the data in its local storage or by proving that the data will be discarded to make space for other highly requested data.

C. The Reputation Module

The reputation module is responsible for managing reputation ratings. A reputation rating $\mathcal{R}_{ij}$ is updated (*i*) when first-hand information is updated, and (*ii*) when received second-hand

[1]Please note that, the routing problem only considers one type of data, i.e., contents, meanwhile the caching problem considers both types of data, i.e., queries and contents.

information (or recommendation) is considered valid to be incorporated.

If store and forward first-hand information that are kept by each vehicle are available, they are combined to form a unique first-hand information, hereafter called first-hand information $\mathcal{F}_{ij} = (\alpha, \beta)_{\mathcal{F}}$ as follows:

- If $(\alpha_s > \alpha_f$ and $\alpha_f = 1$ and $\alpha_s > \chi)$ then $\alpha_{\mathcal{F}} = \alpha_f$ and $\beta_{\mathcal{F}} = \beta_{\mathcal{F}} + 1$. χ represents the number of evidence of stored (or cached) data a node has while not having any evidence of data that the node forwarded (or disseminated) of another node.
- Otherwise, $\alpha_{\mathcal{F}} = \alpha_f$ and $\beta_{\mathcal{F}} = \beta_f$.

The first-hand information rating corresponds to the expectation of $Beta(\alpha, \beta)_{\mathcal{F}}$ and is computed using Eq. 4.

When first-hand information is updated, an exponential weighted moving average (EWMA) is used to update the reputation rating, therefore, allowing for reputation fading as follows

$$\mathcal{R}_{ij}^{t} = (1 - \phi)\mathcal{R}_{ij}^{t-1} + \phi\mathcal{F}_{ij}^{t} \tag{6}$$

where ϕ is the smoothing factor and $0 < \phi < 1$.

Since classical EWMA averages do not take into account time, at the end of a given time window, first-hand information is updated by means of the fading mechanism as explained in Section IV-A.

D. The Trust Module

The goal of the trust module is to provide a dynamic computation model for effectively evaluating the trust among nodes in the presence of highly oscillating malicious behavior such as gray-hole attacks. It is assumed that node v_i (called the evaluator node) needs to calculate the trustworthiness of node v_k (called the target node). This is performed when v_i receives first-hand information from some node v_k about node v_j.

First, a similarity metric is computed aiming at determining to what extent nodes v_i and v_k are alike. The similarity metric consists in calculating the personalized difference in first-hand information ratings over a common set of interacting nodes. Let H_i represent the set of nodes with whom v_i interacted. Then, $H_{i \cap k} = H_i \cap H_k$ denotes the set of nodes with whom both nodes v_i and v_k interacted. The personalized similarity metric (ζ_{ik}) is given by

$$\zeta_{ik} = 1 - \sqrt{\frac{\sum_{a \in H_{i \cap k}} \left(\mathcal{F}_{ia} - \mathcal{F}_{ka}\right)^2}{|H_{i \cap k}|}} \tag{7}$$

Any node k's recommendations towards j are synthesized at i as follows

节点k向节点i推荐节点j

$$\mathcal{S}_{ij}^{t} := \mathcal{F}_{ij,k}^{t} = (1 - \phi)\mathcal{S}_{ij}^{t-1} + \phi\mathcal{F}_{kj}^{t} \tag{8}$$

In addition, the variance (σ) between received and stored second-hand information and the personalized similarity metric are also synthesized.

$$\sigma^{t} = (1 - \psi) \cdot \sigma^{t-1} + \psi \cdot \mathcal{D}^{t}$$
$$\mathcal{D} = \mathcal{F}_{kj} - \mathcal{S}_{ij} \tag{9}$$

Algorithm 1: K-Means Clustering.

Data: Similarity observations: $o_i \in \mathcal{O}$
Result: Clusters: $\mathcal{S}_i, i = 1, \cdots, K$
Initialize $s_k, k = 1, \cdots, K$ cluster centers using the Forgy method [29];
while s_k *does not converge* **do**
  foreach $o_i \in \mathcal{O}$ **do**
    $S_i^* = \underset{k}{\operatorname{argmin}}\ d(o_i, s_k)$
  end
  for $s_k, k = 1, \cdots, K$ **do**
    $s_k = \frac{1}{|\mathcal{O}_k|} \sum_{i}^{|\mathcal{O}_k|} o_i$
  end
end

where $0 < \psi < 1$. Let a similarity observation o_i of node v_i be a tuple composed of node v_k that sent the recommendation and the personalized similarity metric ζ_{ik} between nodes v_i and v_k, i.e, $o_i =< v_k, \zeta_{ik} >$. Let $\mathcal{S}_i, \{i = 1, \ldots, K\}$ denote a set of K clusters. Let $s_k, \{k = 1, \ldots, K\}$ denote cluster centers. Since binary classification problems will be considered (see Section IV-E), K is set to 2. As more recommendations are received, node v_i applies the K-Means algorithm (Algorithm 1) to cluster the nodes that sent recommendations based on their similarity. Let $\mathcal{S}_i^+$ denote the cluster with the highest value of cluster center. Recommendations are incorporated as follows

$$\mathcal{R}_{ij}^{t} = \frac{\mathcal{R}_{ij}^{t-1} + \mathcal{F}_{kj}^{t} \cdot \zeta_{ik} \cdot \epsilon}{1 + \zeta_{ik} \cdot \epsilon}$$
$$\epsilon = \begin{cases} 1, & \text{if node } v_k \in \mathcal{S}_i^+ \\ \frac{\mathcal{D}^t}{\mathcal{D}_{\max}}, & \text{otherwise} \end{cases} \tag{10}$$

where ϵ is the discount factor and $\mathcal{D}^t$ is the current variance and $\mathcal{D}_{\max}$ is the maximum variance ever obtained, and $\mathcal{D}_{\max} > \mathcal{D}^t$.

The synthesization of second-hand information and of the variance between received and stored second-hand information in conjunction with the personalized similarity metric make the framework resilient against false praise and accusation performed by colluding gray-hole misbehaving nodes.

E. The Decision Module

The decision module is responsible for classifying vehicles in the system regardless of the problem at hand, e.g., routing, caching or both. Classification aims to learn a mapping from inputs $\mathbf{x}$ to outputs $c(\mathbf{x})$, where $c \in \{1, \ldots, C\}$, with C being the number of classes.

1) Bayesian Classification: In Bayesian classification problems, Θ is discrete and the goal is to estimate θ given an observed data x. To address the routing and caching problems, the vehicle's behavior classification problem was considered. Let

- $\theta \in \Theta = \{\theta_0 = \text{NORMAL}, \theta_1 = \text{MISBEHAVING}\}$ unknown state of nature.
- $X \in \mathcal{X}$ be a random variable with $\{f(x|\theta), x \in X\}$
- $\pi(\theta) > 0$ and $\sum_{\theta \in \Theta} \pi(\theta) = 1$ be the prior probability mass function.

- $a \in \mathcal{A} = \{a_0 = \text{CACHE\_FORWARD}, a_1 = \text{DO\_NOT\_CACHE\_FORWARD}\}$[2] be the allowed decision or action.
- The "0/1" loss function be used for classification. It assigns zero cost to any correct decision and unit cost to any wrong decision.
- $\mathcal{D}$ be the set of allowed decision rules. A decision rule $(\delta(x))$ specifies how actions or decisions are chosen given x.
- $L(\theta, a)$ be the loss function. It quantifies the consequences of the decisions.

$$L(\theta, a) = \begin{cases} 1, & \begin{cases} \text{if } \theta = \theta_0 \text{ decide } a = a_1 \\ \text{if } \theta = \theta_1 \text{ decide } a = a_0 \end{cases} \\ 0, & \text{otherwise} \end{cases} \tag{11}$$

The optimal Bayesian decision is given by

$$\begin{aligned} \delta_{\text{Bayes}}(x) &= \underset{a \in \mathcal{A}}{\text{argmin}}\, \rho(\pi(\theta), a|x) \\ &= \underset{a \in \mathcal{A}}{\text{argmin}}\, (L(\theta_0, a) f(x|\theta_0) \pi(\theta_0) \\ &\quad + L(\theta_1, a) f(x|\theta_1) \pi(\theta_1)) \end{aligned} \tag{12}$$

$$\delta_{\text{Bayes}}(x) = \begin{cases} \theta_0, & \text{if } l(x) \geq t \\ \theta_1, & \text{otherwise} \end{cases} \tag{13}$$

where $l(x) = \frac{f(x|\theta_0)}{f(x|\theta_1)}$ is the likelihood ratio and $t = \frac{\pi(\theta_1)}{\pi(\theta_0)}$ is the decision threshold.

The likelihood function is given by the Bernoulli distribution $f(x|\theta) = \theta^r (1-\theta)^{n-r}$, where $r = \sum_{i=0}^{n} x_i$, and r denotes the number of outcomes representing correct behavior.

In the beginning, if the only information available is the conditional probability density function of the observed data given the θ, the maximum likelihood decision criterion (δ_{ML}) [30] is used. δ_{ML} is defined as

$$\delta_{\text{ML}} = \begin{cases} \theta_0, & \text{if } l(x) \geq 1 \\ \theta_1, & \text{otherwise} \end{cases} \tag{14}$$

In the vehicle's behavior classification problem, after each interaction between two nodes, the sender updates the reputation rating of the other node based on the result of this interaction. Each node clusters the other nodes to whom it interacted in two groups: normal nodes, e.g., if $\mathcal{R}_{ij} \geq 1/2$, and misbehaving nodes, e.g., if $\mathcal{R}_{ij} < 1/2$. The prior probabilities $\pi(\cdot)$ of these clusters, which allow determining the decision threshold, are coefficients of the convex combination of the number of nodes in these clusters. The optimal Bayesian decision is computed using Eq. 13 given the prior probabilities. However, if a correct behavior is observed and $\pi(\theta_1) > \pi(\theta_0)$, one may incur in false positives, i.e., a misclassification, while using the optimal Bayesian decision criterion, because of the higher weight of the decision threshold in comparison to the likelihood ratio. The workaround consists in finding attenuation parameters $\hat{\alpha}$ and $\hat{\beta}$ of the *posterior mean Bayesian estimator* $\left(\hat{\theta}_{\text{PM}}\right)$ [30] and computing an attenuated decision threshold. $\hat{\theta}_{\text{PM}}$ is given by

$$\hat{\theta}_{\text{PM}} = \frac{\hat{\alpha} + r}{\hat{\alpha} + \hat{\beta} + n} \tag{15}$$

For the minimum possible case, i.e., one correct behavior being observed and two clusters, one with 2 misbehaving nodes and the other with 1 normal node, $l(x)$ is $4/3$. By combining the latter with Eq. 13,

$$t = \frac{1 - \hat{\theta}_{\text{PM}}}{\hat{\theta}_{\text{PM}}} \leq \frac{4}{3}$$

$$\hat{\theta}_{\text{PM}} \geq 3/7 \tag{16}$$

The Bayesian attenuation parameters $\hat{\alpha}$ and $\hat{\beta}$, which result from Eqs. 15 and 16, are given by

$$\begin{aligned} &\underset{\hat{\alpha}, \hat{\beta} > 0}{\text{argmin}}\, f(\hat{\alpha}, \hat{\beta}) \geq 0 \\ &f(\hat{\alpha}, \hat{\beta}) = 7r + 4\hat{\alpha} - 3(\hat{\beta} + n) \end{aligned} \tag{17}$$

If, for the case above, $\hat{\alpha} = \hat{\beta} = 2$ than $t = l(x)$. If instead the *maximum a posteriori Bayesian estimator* [30] was used, $t > l(x)$ which would lead to misclassification.

2) Nearest Neighbor Classification: In a classification problem, each input $\mathbf{x}$ is a tuple composed of the node v and a reputation rating $\mathcal{R}$ that was updated using the trust module, i.e, $\mathbf{x} = < v, \mathcal{R} >$, That have a matching class label $c \in \{\text{NORMAL}, \text{MISBEHAVING}\}$. Let $\mathcal{D} = \{\mathbf{x}^n, c^n\}, n = 1, \ldots, N$ be a training set. Given a new $\mathbf{x}$, the goal is to find the right class $c(\mathbf{x})$. The training set can be obtained by means of Bayesian classification (as explained in Section IV-E1). An easy approach for this learning problem is defined as follows: for a new $\mathbf{x}$, find in the training set the nearest input and use its class (Algorithm 2).

Algorithm 2: The nearest neighbor algorithm to classify $\mathbf{x}$ given train data $\mathcal{D}$.

Data: $\mathbf{x}, \mathcal{D}$
Result: $c(\mathbf{x})$
foreach $x \in \boldsymbol{x}^n$ **do**
  calculate $d^n = d(\mathbf{x}, x)$;
end
find x^* that is nearest to $\mathbf{x}$: $n^* = \underset{n}{\text{argmin}}\, d^n$;
Assign the class label $c(\mathbf{x}) = c^{n^*}$

F. The Bio-Inspired Mechanism

Vehicles use V2X communications to learn about significant events in the network. However, neighboring vehicles might misbehave by reporting incorrect information in order to take advantage of the system. In addition, misbehaving nodes may also provide incorrect recommendations about other nodes in

[2]Instead of representing distinct actions such as $a_0 =$ CACHE for the caching problem and $a_0 =$ FORWARD for the routing problem, it is represented only one action $a_0 =$ CACHE_FORWARD for simplicity. The same applies to a_1.

order to influence the receiver's decision. The existence of incorrect information and misbehaving vehicles render the system unreliable for safety and emergency applications. In addition, one of the main challenges in network security is determining the difference between normal and potentially harmful activity. This problem is exacerbated by current and future threats that require the development of automated and adaptive mechanisms.

The mechanisms proposed in previous sections allow the framework to identify correctly the events as well as misbehaving nodes in most cases. However, content dissemination applications are also characterized by fewer interactions between nodes because of cache hits conversely to routing. In most cases, this increases misbehavior detection time.

The proposed biologically inspired (i.e., bio-inspired) mechanism is based on Danger Theory and works as follows: at the end of each timeslot τ_k, node v_i randomly selects a node v_j in its vicinity that it has evidence or suspects to be misbehaving. For example, v_j could be selected if it has $\alpha_f = 1$ and $\alpha_s > \chi$ that is seen by the framework as a danger signal. In that case, v_i generates a decoy message using a backoff algorithm [31] destined to v_k that it considers having a good behavior, that is, having a good reputation. The decoy message can only be forwarded at most twice (i.e., the danger zone centered at v_i) and is intended to test if v_j is, in fact, a misbehaving node. If v_j is de-facto misbehaving, it will not forward the message to v_k. Otherwise, it will forward and v_k will generate an SFM destined to v_i. The following backoff algorithms were considered for the generation of decoy messages: Binary Exponential Backoff (BEB) and Multiplicative Increase Linear Decrease (MILD). Backoff algorithms are employed by the IEEE 802.11 Distributed Coordination Function [32] to share the medium.

Our BEB algorithm works as follows: after a successful decoy transmission attempt $\mathfrak{t}$ at time $t \in \tau_k$ by v_i to v_k about v_j, v_i selects a random slot $\mathfrak{r}$ between 0 and $2^{\mathfrak{t}} - 1$. The next decoy message about v_j from v_i would only be generated at time $t' \in \tau_k \times \mathfrak{r}$. On the other hand, in our MILD algorithm, the next decoy message about v_j from v_i would only be generated at time $t' \in \tau_k \times \mathfrak{m}$, where $\mathfrak{m} \in \mathbb{N}$ is a multiplicative factor.

V. Performance Evaluation

This section presents the simulation model and results regarding the performance evaluation of ReFIoV.

A. The Simulation Model

ReFIoV was implemented on the Opportunistic Network Environment (ONE) simulator [33]. The simulation model consisted of synthetic mobility models (SMM) and a real mobility trace (RMT). The simulation time was 14 and 7 days with an update interval of 1.0 s for SMM and RMT scenarios, respectively. The smoothing factor (ϕ) and ψ were set to 0.15 and 0.25. ϕ is close to the α value used in the estimation of the Round Trip Time (RTT) on the Transport Control Protocol (TCP) [32], and ψ is equal to the β value. The fading factor (η) was set to 0.95 because VDTNs are normally sparse and this value allows forgetting gradually old first-hand information. χ was set to 3. The latter parameter represents the number of evidence of store (or cached) data by a node meanwhile not having any evidence of data forwarded (or disseminated) by the same node to another one. Higher values of χ will slow the convergence of ReFIoV.

The vehicles misbehavior considered for evaluation were black- and gray-hole attacks. It was considered that nodes implementing gray-hole attacks were also colluding. The effects of vehicles' misbehavior were examined considering that vehicles were using Epidemic to forward (or disseminate) data. However, for the caching problem, it was also considered that vehicles were using an on-path caching approach with a Least-Frequently Used (LFU) policy. The percentage of misbehaving vehicles varied from 20% to 80% with increments of 20%.

The size of vehicles' local storage was 256 MB. The mobile data contents' size varied from 50 KB to 1.5 MB. The following mobile data generation rates were considered: randomly every 1.25 to 2.5 minutes – 1.25–2.5 min (DG1), 2.5–5 min (DG2) and 5–10 min (DG3). They were used for data content and query generation for the routing and caching problems, respectively. In addition, for the caching problem, the query generation followed the Zipf distribution [34]. The latter distribution is commonly used for the characterization of the popularity of objects. Queries were made to 5 and 10 content servers for SMM and RMT scenarios, respectively. Each content server stored 50 contents.

1) Synthetic Mobility Models: The simulation time was 14 days with an update interval of 1.0 s. Map-based mobility models of Helsinki city over an area of 4.5 × 3.4 Km and Barcelona city over an area of 12 × 12 Km were used. It was assumed that all nodes used Bluetooth and Wi-Fi interfaces. Given that Helsinki and Barcelona cities are urban areas, the communication range between nodes was 10 m and the communication was bidirectional at a constant transmission rate of 2 Mbit/s for the Bluetooth interface. Only two nodes within range can communicate with each other at a time. The TTL attribute of each data content was 5 h. The following mobility models were considered:

a) Shortest-path map-based movement (SPMBM): SPMBM [22] consisted of a network with 144 vehicles and 6 trams in Helsinki city. Vehicles were moving at a speed varying between 2.7 to 13.9 m/s. Each time a vehicle reaches its destination, it paused for 60 to 300 s. Given that Helsinki city is an urban area, the communication range between nodes was set to 10 m and the communication is bidirectional at a constant transmission rate of 10 Mbit/s for the 802.11a Wi-Fi interface.

b) Map-based movement (MBM): MBM [35] consisted of a network with 90 vehicles, 30 pedestrians and 6 RSUs in Barcelona city. Vehicles and pedestrians were moving at a speed varying between 2.7 to 13.9 m/s and 0.5 to 1.5 m/s, respectively. Each time a vehicle reaches its destination, it paused for 60 to 300 s. Given that Barcelona city is an urban area, the communication range between nodes was set to 30 m and the

communication is bidirectional at a constant transmission rate of 6 Mbit/s for the 802.11a Wi-Fi interface. The size of the local storage of pedestrians and RSUs was 256 and 512 MB, respectively.

2) Real Mobility Trace: The taxicabs in Rome (TR) [36] traces contains Global Positioning System (GPS) coordinates of approximately 320 taxicabs collected over 30 days in Rome, Italy. The simulation duration and number of vehicles were reduced to 7 days and 304 vehicles, respectively. It was assumed that all nodes used an 802.11p Wi-Fi interface with a communication range of 100 m and a communication speed of 10 Mbit/s. The TTL attribute of the mobile data was 24 h.

B. Simulation Results

The evaluation of the performance of ReFIoV consisted in appraising the reputation, trust and decision modules. For each setting, i.e., protocol-percentage pair, up to five independent simulations using different data generation seeds were conducted, and the results averaged, for statistical confidence.

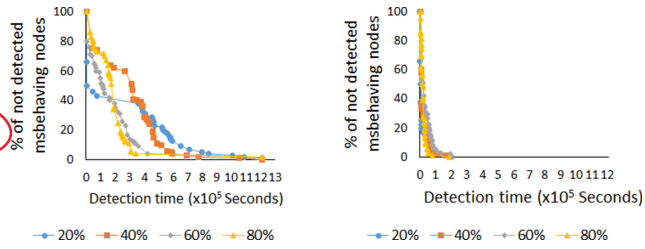
ReFIoV, which uses an Epidemic dissemination approach, was compared to [22] (hereafter *r*REPSYS) and [1] (hereafter *c*REPSYS), which are state-of-the-art reputation systems.

The following main metrics are considered for the evaluation of ReFIoV:

- *Detection time of misbehaving vehicles* corresponds to the simulation time that took all normal vehicles to classify correctly all misbehaving vehicles they came in contact with, starting at the detection instant of the first misclassification.
- *Robustness* against false negatives and positives. The following metrics were defined:
  - Vehicle's Behavior False Positives Ratio (VBFPR) is the number of misbehaving vehicles with a good classification, i.e., classified as CACHE_FORWARD, overall vehicles classified.
  - Vehicle's Behavior False Negatives Ratio (VBFNR) is the number of normal vehicles with a bad classification, i.e., classified as DO_NOT_CACHE_FORWARD, overall vehicles classified.
- *Control messages' overhead ratio,* which is the ratio between the number of control data of the proposed scheme (i.e., SFM and decoy messages disseminated) overall data.

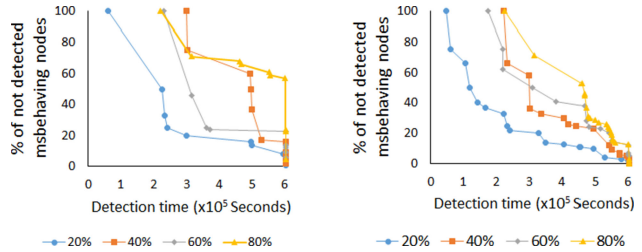
The influences of using different data generation rates and the reputation decay mechanism, which allows redemption of misbehaving nodes, both in the presence of black-hole misbehaving nodes were analyzed. In addition, the influence of using second-hand information to enhance detection time of colluding gray-hole misbehaving nodes was also analyzed.

1) Detection Time of Misbehaving Vehicles: First, the routing problem is analyzed. Fig. 3 presents the time necessary for each normal node with ReFIoV and *r*REPSYS to classify correctly all misbehaving nodes they meet as DO_NOT_CACHE_FORWARD in the SPMBM scenario for the black-hole attack. ReFIoV was only using the reputation and decision modules, i.e., Bayesian learning and classification and the



(a) *r*REPSYS (b) ReFIoV

Fig. 3. The time necessary for *r*REPSYS and ReFIoV to classify correctly misbehaving vehicles as DO_NOT_CACHE_FORWARD for 20, 40, 60, and 80% of black-hole vehicles using DG3 in the SPMBM scenario.



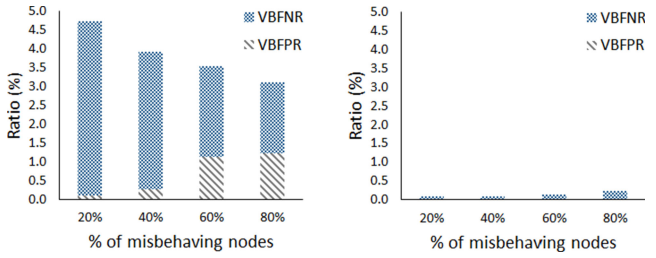
(a) *c*REPSYS (b) ReFIoV

Fig. 4. The time necessary for *c*REPSYS and ReFIoV to correctly classify misbehaving vehicles as DO_NOT_CACHE_FORWARD for 20, 40, 60, and 80% of black-hole vehicles using DG1 in the TR scenario.

bio-inspired mechanism, meanwhile *r*REPSYS was using all its modules. Each point on the graph corresponds to the average of the percentage of misbehaving nodes that were misclassified, i.e., classified as CACHE_FORWARD, from the perspective of each normal node in the network at a given time instant. The sampling was performed every 60 s.

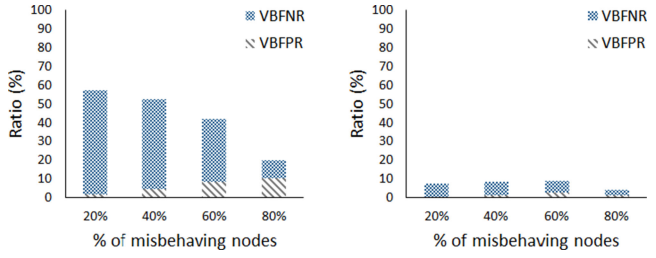
*r*REPSYS takes more time to correctly classify misbehaving nodes, which can be confirmed by the long tail in all its curves (see Fig. 3(a)). A long tail means that there is a considerable number of normal nodes with a small percentage of misclassified misbehaving nodes. Consider, for instance, the tails of the curves representing 80% of misbehaving nodes in Fig. 3 for ReFIoV and *r*REPSYS. ReFIoV presented the shortest tail, which shows that it was much faster to correctly classifying misbehaving nodes. If the other curves are compared, ReFIoV was also much faster if compared with *r*REPSYS mostly because of the bio-inspired mechanism. The decoy messages were essential in reducing detection time. In short, ReFIoV is approximately 9.4, 7.8, 7.5 and 4.9 times faster in comparison to *r*REPSYS to detect 20, 40, 60 and 80% of misbehaving nodes, respectively.

Lastly, the caching problem is analyzed. Fig. 4 presents the time necessary for each normal node using *c*REPSYS and ReFIoV to classify correctly all misbehaving nodes they meet as DO_NOT_CACHE_FORWARD in the TR scenario. In the detection time of the routing problem (Fig. 3(b)), each node using ReFIoV analyze based on each data content message that it forwards, the behavior of other nodes with whom it interacts, that is, if they store and forward these data content messages.



(a) rREPSYS (b) ReFIoV

Fig. 5. Vehicle's behavior false positives and negatives ratios for 20, 40, 60, and 80% of black-hole vehicles using DG3 for the routing problem in SPMBM.



(a) cREPSYS (b) ReFIoV

Fig. 6. Vehicle's behavior false positives and negatives ratios for 20, 40, 60, and 80% of black-hole vehicles using DG1 for the caching problem in TR.

Conversely, in the caching system, the analysis made at each node is based on data query and content messages, that is, if another node stores and forwards data query messages, and/or if this other node cache and disseminate data content messages. Besides the latter, only a limited number of contents is considered in the caching problem, and as time passed these contents get cached in intermediate nodes reducing even further the interaction between normal and misbehaving nodes. These are the sole reasons for the behavior of the curves in Fig. 4. However, if a considerable higher number of different contents exist at each content server, then the caching problem would become similar to the routing problem, hence presenting also similar detection times.

By analyzing Fig. 4, one may conclude that ReFIoV performed better than cREPSYS. This was due to the dissemination approach used that always attempted to replicate a content to a recently encountered node.

2) Robustness: Similarly to the previous section, the routing problem is analyzed first. In Fig. 5, two metrics, namely VFPR and VFNR, are considered to measure the robustness against black-hole attacks in the SPMBM scenario. The main goal of any reputation system is to classify nodes taking into account their behavior hence identifying and isolating misbehaving nodes. ReFIoV achieved this goal since it presents negligible (i.e., below 0.3%) VFPRs and VFNRs. In fact, VFPR was below 0.02%, conversely to rREPSYS whose VFPR increased with the increase in the percentage of misbehaving nodes. However, this came at a cost as ReFIoV presents additional control overhead because of the bio-inspired mechanism as explained in Section V-B5. Nevertheless, in the eventuality of misclassified normal nodes being temporarily isolated from the network, they will be able to rejoin it due to the fading mechanism.

One may also conclude, based on Fig. 5(b), that the robustness of rREPSYS improves with the increase of the number of misbehaving nodes. Please note that by varying the number of misbehaving nodes, the total number of nodes remains the same. Consequently, an inferior number of normal nodes interacted more with an increasing number of misbehaving nodes, which enabled a faster detection.

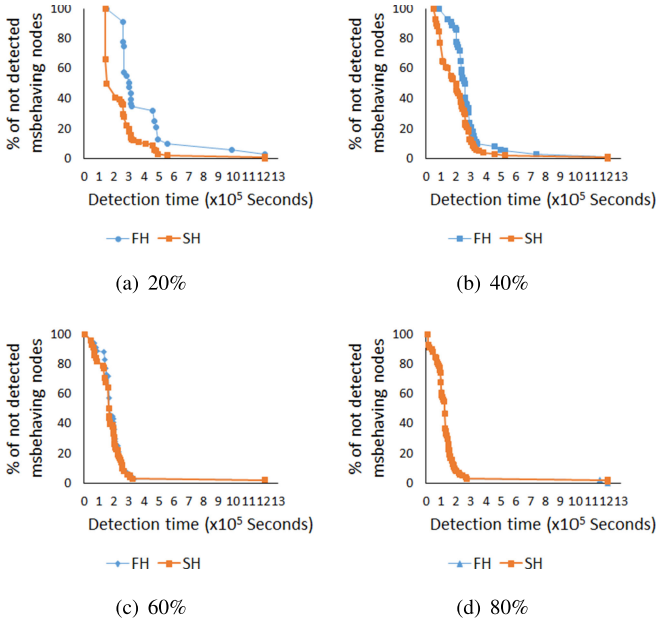
Fig. 6 presents the robustness of cREPSYS and ReFIoV for the caching problem in the TR scenario in the presence of black-hole misbehaving nodes. Differently from routing where a data message is forwarded between a source and a destination node using the delay-tolerant networking paradigm, in the information-centric networking paradigm, requested data contents can be returned by nodes having these contents in their local storage. This reduced interactions among nodes hence increasing detection time and VFNRs. The bio-inspired mechanism enabled reducing even further ReFIoV's false positives by allowing each node to randomly test other nodes with whom it interacted having α_s values closer to χ. The latter mechanism aimed at increasing the interaction among nodes hence allowing to differentiate even better normal nodes from misbehaving ones.

TABLE I
REFIOV WITH DG1 LOSSES (-) AND GAINS (+) IN COMPARISON TO OTHER DATA GENERATION RATES FOR THE TR SCENARIO

% misbehaving nodes	DG2		DG3	
	VFPR	VFNR	VFPR	VFNR
20%	-35.79	0.45	-72.11	0.72
40%	-25.60	-0.10	-66.38	0.54
60%	-23.82	-0.06	-56.79	0.66
80%	-13.42	-14.62	-25.93	-26.89

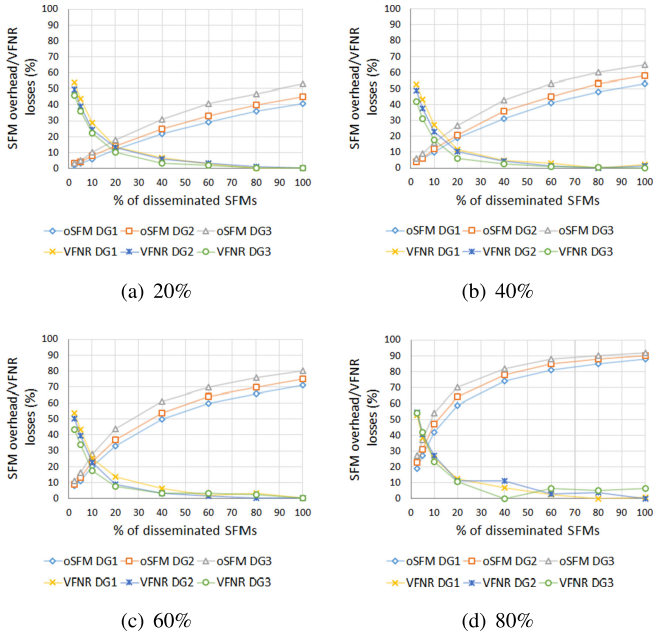
3) The Influences of the Data Generation Rate and the Reputation Decay Mechanism: The influence of the data generation rate on ReFIoV without the bio-inspired algorithm is analyzed in the TR scenario. Table I presents robustness gains (+) and losses (−) of ReFIoV with DG1 in comparison to ReFIoV with DG2 and DG3. These results show that the performance of ReFIoV was influenced by the data generation rate. Ideally, only one evidence should be sufficient to identify a misbehaving node. However, to avoid misclassifications, more evidence is necessary even though it is assumed that nodes' behaviors do not change over time for the black-hole attack.

Now, the influence of the reputation decay mechanism of ReFIoV also without the bio-inspired algorithm is analyzed. The goal of the decay mechanism, as explained in Section IV-C, is to enable redemption, that is, to allow misclassified normal nodes to rejoin the network as their reputation fades. Overall, the performance of ReFIoV with the decay mechanism slightly degraded if compared to the unrealistic case where the mechanism was not used. It was also noticed that the selection of the decay interval should take into account the data generation rate, being directly proportional to this rate. The selection of the decay time window should preferably be addressed as an



(a) 20% (b) 40% (c) 60% (d) 80%

Fig. 7. Comparison of detection times between ReFIoV with first-hand (FH) and second-hand (SH) information for 20, 40, 60, and 80% of colluding vehicles performing a gray-hole attack using DG3 in the SPMBM scenario.



(a) 20% (b) 40% (c) 60% (d) 80%

Fig. 8. SFM messages overhead (oSFM) and VFNR losses for different percentages of disseminated SFM messages and mobile data generation rates, and for different percentages (20, 40, 60 and 80%) of vehicles performing a black-hole attack in the MBM scenario.

optimization problem aiming at improving the overall performance of the system, thus not being the case of one-solution-fits-all.

4) The Influence of Second-Hand Information: Up until now, only the back-hole attack was considered. Fig. 7 presents a comparison of the detection times between ReFIoV with first-hand (FH) and second-hand (SH) information for 20, 40, 60 and 80% of colluding vehicles performing a gray-hole attack using DG3 in the SPMBM scenario. The goal now is to appraise the trust module hence evaluating the influence of integrating second-hand information. Please note that the bio-inspired mechanism was not considered here.

One may conclude from Fig. 7 that the use of second-hand information reduces detection time. However, the gains attained by using second-hand information reduce with the increase in the percentage of misbehaving nodes. The main reason behind this is that ReFIoV requires interactions among nodes to classify them and these interactions increase as more misbehaving nodes are added to the network. Recall that second-hand information corresponds to first-hand information sent by another node, i.e., a previous interaction between two other nodes, and it is incorporated by considering how similar the opinions of the sender and receiver of second-hand information are in view of their common set of neighbors. The use of the personalized similarity metric in conjunction with the synthesization of information allowed ReFIoV to be resilient against colluding gray-hole misbehaving nodes, that is, misbehaving nodes that behave in an unpredictable manner by oscillating their behavior to conceal their true nature.

5) Control Messages' Overhead Ratio:

a) The SFM's overhead ratio: Fig. 8 presents the control overhead caused by SFM messages overall disseminated messages and the VFNR losses by considering a probabilistic dissemination of SFM messages with probabilities varying from 2.5% to 100% (in which, the latter value corresponds to disseminating all SFM messages). The goal of probabilistically disseminating SFM messages was to reduce the number of such messages in the network. VFNR losses were obtained by comparing VFNR values attained with SFM messages disseminated with different probabilities.

The control overhead caused by SFM messages increased (*i*) as more SFM messages were disseminated, and (*ii*) with the reduction of the data generation rate. The former was due to a higher number of SFM messages in the network that also occupied more local storage space. In the latter, less data replicas were created as a result of the reduction of the data generation rate. However, the number of replicas of each data content also increased.

In general, VFNR losses reduced considerably with the increase in the number of SFM messages disseminated and reduced slightly with the reduction of the data generation rate. This shows that SFM messages are necessary but their dissemination should be done with care thus avoiding to saturate the network too many control messages.

Moreover, the average storage occupancy time (ASOT), which measures the average amount of time each data content stayed in the local storage, presented a similar behavior to the control overhead. Specifically, ASOT (see Fig. 9) increased considerably with the reduction of the data generation rate, and increased slightly with the increase of the probability of the dissemination of SFM messages. Finally, yet importantly, ASOT reduced with the increase of the percentage of misbehaving

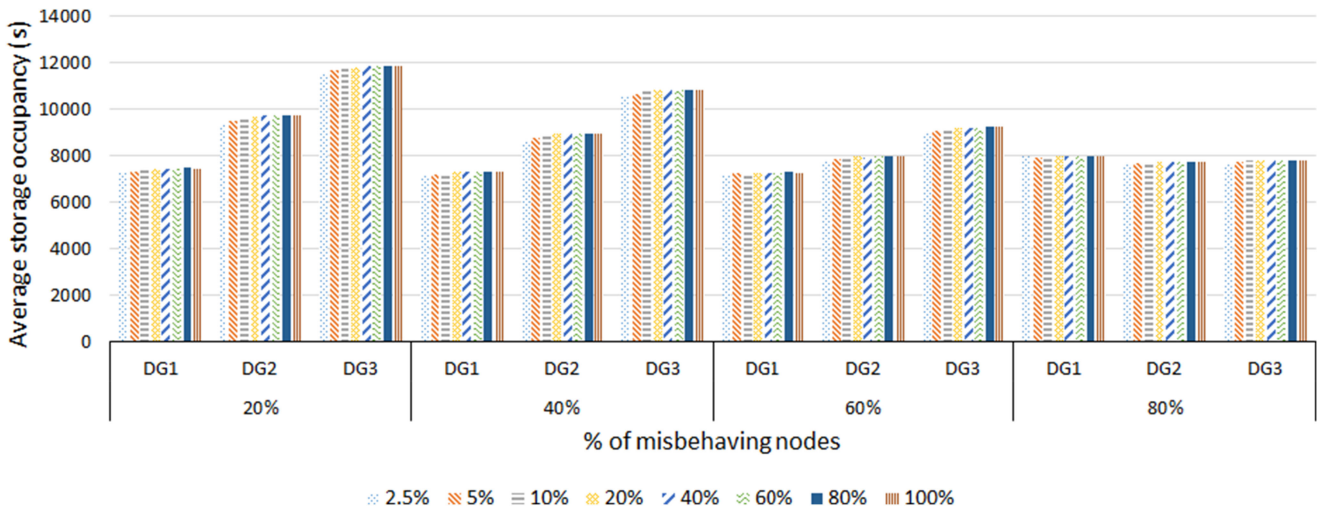


Fig. 9. The average storage occupancy time for different percentages of disseminated SFM messages and mobile data generation rates, and for different percentages (20, 40, 60, and 80%) of vehicles performing a black-hole attack in the MBM scenario.

TABLE II
THE OVERHEAD RATIO CAUSED BY THE BIO-INSPIRED MECHANISM FOR THE BACKOFF ALGORITHMS CONSIDERED ON SPMBM SCENARIO

% misbehaving nodes	BEB	MILD2	MILD3	MILD4
20%	1.61	1.85	2.11	1.71
40%	2.01	2.32	2.57	2.73
60%	3.00	3.00	3.13	3.01
80%	2.23	2.60	2.23	2.23

TABLE III
THE OVERHEAD RATIO CAUSED BY THE BIO-INSPIRED MECHANISM FOR THE BACKOFF ALGORITHM CONSIDERED ON TR SCENARIO

% misbehaving nodes	BEB	MILD2	MILD3	MILD4
20%	3.38	3.72	3.88	3.75
40%	4.33	4.88	4.77	4.88
60%	4.78	6.23	5.84	6.73
80%	5.03	7.22	6.55	6.23

nodes given that the fewer remaining good nodes disseminated less SFM messages.

b) The bio-inspired mechanism's overhead ratio: Despite the advantages presented by the use of the bio-inspired mechanism, such as low detection times of misbehaving nodes, its use also entails some disadvantages, such as additional control overhead due to the use of decoy messages. Though, the use of backoff algorithms to generate decoy messages enabled the mechanism to present low control overhead if compared to the algorithms used to forward (or disseminate) data. Table II and III present the control overhead ratio caused by the mechanism in both scenarios. The following backoff algorithms were considered: BEB and MILD. Different multiplicative increase factors were considered in MILD, namely 2 (MILD2), 3 (MILD3) and 4 (MILD4).

By analyzing both tables, one may conclude that BEB presents the lowest overhead despite the gains in comparison to other approaches, namely MILD2, MILD3, and MILD4, not being very high. In addition, ReFIoV with BEB also performed better than other backoff algorithms for the main metrics considered in this Section.

VI. CONCLUSIONS AND FUTURE WORK

In this article, a novel reputation framework for information-centric vehicular applications such as content dissemination, which leverages ML and AIS was proposed.

The emerging latency requirement of 5G-based vehicular networks relies on the cooperative behavior of vehicles. ReFIoV plays an important role by efficiently providing incentives for vehicles to start sharing their resources by storing (or caching) and forwarding (or disseminating) other vehicles' data thus reducing latency to the users that requested the data. The performance evaluation has shown that ReFIoV's detection time is at most 9 times faster, and it presents negligible and very low false positives and negatives in comparison with other reputation systems for both routing and caching problems, respectively. Routing and caching are two distinct problems even in I^2oV since on the latter problem, data queries do not always need to reach the content server. This implies that fewer messages circulate in the network which increases detection time of misbehaving nodes. The use of second-hand information allowed ReFIoV to be resilient against colluding misbehaving nodes behaving in an unpredictable manner by changing their behavior to conceal their true nature.

As future work, the following research challenges have been identified: (i) the evaluation of ReFIoV with other caching policies and forwarding mechanisms, (ii) the use of more elaborate attacker scenarios.

REFERENCES

[1] N. Magaia, Z. Sheng, P. Pereira, and M. Correia, "REPSYS: A robust and distributed incentive scheme for collaborative caching and dissemination in content-centric cellular-based vehicular delay-tolerant networks," *IEEE Wireless Commun. Mag.*, vol. 25, no. 3, pp. 65–71, Jun. 2018.

[2] P. R. Pereira, A. Casaca, J. J. P. C. Rodrigues, V. N. G. J. Soares, J. Triay, and C. Cervello-Pastor, "From delay-tolerant networks to vehicular delay-tolerant networks," *IEEE Commun. Surv. Tut.*, vol. 14, no. 4, pp. 1166–1182, Oct.–Dec. 2012.

[3] N. Benamar, K. D. Singh, M. Benamar, D. E. Ouadghiri, and J.-M. Bonnin, "Routing protocols in vehicular delay tolerant networks: A comprehensive survey," *Comput. Commun.*, vol. 48, pp. 141–158, 2014.

[4] K. Pentikousis *et al.*, "Information-centric networking: Baseline scenarios," *Internet Res. Task Force, RFC* 7476, 2015. [Online]. Available: https://tools.ietf.org/html/rfc7476

[5] N. Magaia, P. R. Pereira, and M. P. Correia, "Selfish and malicious behavior in Delay-Tolerant Networks," in *Proc. Future Network and Mobile Summit*, 2013, pp. 1–10.

[6] N. Magaia, P. Pereira, and M. P. Correia, "Security in delay-tolerant mobile cyber physical applications," in *Cyber-Physical Systems: From Theory to Practice*, D. B. Rawat, J. J. P. C. Rodrigues, and I. Stojmenovic, Eds. Boca Raton, FL, USA: CRC Press, 2015, ch. 15, pp. 373–394.

[7] K. P. Murphy, *Machine Learning: A Probabilistic Perspective*. Cambridge, MA, USA: MIT Press, 2012.

[8] U. Aickelin, D. Dasgupta, and F. Gu, *Artificial Immune Systems*. Boston, MA, USA: Springer US, 2014, pp. 187–211.

[9] J. A. Dias, J. J. Rodrigues, and L. Zhou, "Cooperation advances on vehicular communications: A survey," *Veh. Commun.*, vol. 1, no. 1, pp. 22–32, 2014.

[10] J. A. F. F. Dias, J. J. P. C. Rodrigues, F. Xia, and C. X. Mavromoustakis, "A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks," *IEEE Trans. Ind. Electron.*, vol. 62, no. 12, pp. 7929–7937, Dec. 2015.

[11] G. Dini and A. L. Duca , "Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1167–1178, Sep. 2012.

[12] M. Musolesi and C. Mascolo, "CAR: Context-aware adaptive routing for delay-tolerant mobile networks," *IEEE Trans. Mobile Comput.*, vol. 8, no. 2, pp. 246–260, Feb. 2009.

[13] N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks," *Ad Hoc Netw.*, vol. 11, no. 4, pp. 1497–1509, Jun. 2013.

[14] L. Wei, H. Zhu, Z. Cao, and X. Shen, "SUCCESS: A secure user-centric and social-aware reputation based incentive scheme for DTNs," *Ad-Hoc Sensor Wireless Netw.*, vol. 19, no. 1–2, pp. 95–118, 2013.

[15] G. Shafer, *A Mathematical Theory of Evidence*. Princeton, NJ, USA: Princeton Univ. Press, 1976.

[16] L. Wei, Z. Cao, and H. Zhu, "MobiGame: A user-centric reputation based incentive protocol for delay/disruption tolerant networks," in *Proc. IEEE Global Telecommun. Conf.*, 2011, pp. 1–5.

[17] G. Bigwood and T. Henderson, "IRONMAN: Using social networks to add incentives and reputation to opportunistic networks," in *Proc. IEEE Int. Conf. Privacy, Secur., Risk Trust/IEEE Int. Conf. Social Comput.*, Oct. 2011, pp. 65–72.

[18] L. Yao, Y. Man, Z. Huang, J. Deng, and X. Wang, "Secure routing based on social similarity in opportunistic networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 594–605, Jan. 2016.

[19] L. Li, X. Zhong, and Y. Qin, "A secure routing based on social trust in opportunistic networks," in *Proc. IEEE Int. Conf. Commun. Syst.*, Dec. 2016, pp. 1–6.

[20] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 22–32, Jan. 2014.

[21] E. Ayday and F. Fekri, "An iterative algorithm for trust management and adversary detection for delay-tolerant networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 9, pp. 1514–1531, Sep. 2012.

[22] N. Magaia, P. R. Pereira, and M. Correia, "REPSYS: A robust and distributed reputation system for delay-tolerant networks," in *Proc. 20th ACM Int. Conf. Model., Anal., Simul. Wireless Mobile Syst.*, Nov. 2017, pp. 1–5.

[23] N. Magaia, A. P. Francisco, P. Pereira, and M. Correia, "Betweenness centrality in delay tolerant networks: A survey," *Ad Hoc Networks*, vol. 33, pp. 284–305, Jan. 2015.

[24] Y. Li, D. Jin, P. Hui, and S. Chen, "Contact-aware data replication in roadside unit aided vehicular delay tolerant networks," *IEEE Trans. Mobile Comput.*, vol. 15, no. 2, pp. 306–321, Feb. 2016.

[25] J. Owen, J. Punt, and S. Stranford, *Kuby Immunology*. New York, NY, USA: W. H. Freeman, 2013.

[26] E. Alpaydin, *Introduction to Machine Learning*. Cambridge, MA, USA: MIT Press, 2014.

[27] A. C. Davison, *Statistical Models*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[28] N. Magaia, P. R. Pereira, and M. P. Correia, "Nodes' misbehavior in vehicular delay-tolerant networks," in *Proc. Conf. Future Int. Commun.*, May 2013, pp. 1–9.

[29] G. Hamerly and C. Elkan, "Alternatives to the k-means algorithm that find better clusterings," in *Proc. 11th Int. Conf. Inf. Knowl. Manage.*, 2002, pp. 600–607.

[30] M. A. T. Figueiredo, "Lecture notes on Bayesian estimation and classification," Instituto de Telecomunicações, Instituto Superior Técnico, Lisboa, Tech. Rep., 2004.

[31] M. M. Rahaman, K. Ashrafuzzaman, M. S. Chowdhury, and M. O. Rahman, "Performance measurement of different backoff algorithms in IEEE 802.15.4," in *Proc. Int. Conf. Innov. Sci., Eng. Technol.*, Oct. 2016, pp. 1–4.

[32] J. Kurose and K. Ross, *Computer Networking: A Top-Down Approach*. London, U.K.: Pearson, 2012.

[33] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," in *Proc. 2nd Int. Conf. Simul. Tools Techn.*, 2009, paper 55.

[34] C. Imbrenda, L. Muscariello, and D. Rossi, "Analyzing cacheable traffic in ISP access networks for micro CDN applications via content-centric networking," in *Proc. 1st ACM Conf. Inf.-Centric Netw.*, 2014, pp. 57–66.

[35] N. Magaia, C. Borrego, P. Pereira, and M. Correia, "ePRIVO: An enhanced privacy-preserving opportunistic routing protocol for vehicular delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11154–11168, Nov. 2018.

[36] L. Bracciale, M. Bonola, P. Loreti, G. Bianchi, R. Amici, and A. Rabuffi, "CRAWDAD dataset roma/taxi (v. 2014-07-17)," Jul. 2014. [Online]. Available: http://crawdad.org/roma/taxi/20140717

Authors' photographs and biographies not available at the time of publication.